

The Honorable Judge Robert S. Lasnik

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

JOHN HOLCOMB.,

Defendant.

CASE NO. CR21-75-RSL

[PROPOSED] BRIEF OF *AMICI*
CURIAE AMERICAN CIVIL
LIBERTIES UNION AND
AMERICAN CIVIL LIBERTIES
UNION OF WASHINGTON IN
SUPPORT OF DEFENDANT JOHN
HOLCOMB'S MOTION TO
SUPPRESS

TABLE OF CONTENTS

I.	INTRODUCTION & SUMMARY OF ARGUMENT	1
II.	FACTS	2
III.	ARGUMENT	3
A.	Courts must scrupulously apply longstanding Fourth Amendment rules regarding limits on warrants to searches of digital information to ensure that digital searches do not morph into unconstitutional general searches.	3
1.	Computers and other digital devices contain an immense amount of private, sensitive data.	3
2.	The Fourth Amendment requires that warrants to search digital data be scrupulously particular and narrow.	5
a.	Warrants must clearly limit what officers may seize and police searches must be designed to find relevant information whose seizure is supported by probable cause.	5
b.	Adhering to constitutional requirements about overbreadth and particularity is especially important when officers search electronic information.	8
B.	In case after case, courts are imposing limits on warrants in recognition that probable cause to search or seize some data on a digital device cannot justify access to the totality of the device’s contents.	9
1.	Courts can and should impose limitations on the categories of data to be searched on a digital device.	11
2.	Courts can and should limit searches by time frame to ensure they do not expand beyond data relevant to the crime under investigation.	14
3.	Forensic tools make it straightforward for law enforcement to narrow searches by file type, date range, and other limitations that adhere closely to probable cause.	15
C.	Courts have additional options to ensure that overseizures of data are not exploited in ways that give law enforcement a windfall simply because potential evidence is digital in nature.	17
1.	Courts should strictly limit any applications of the plain view doctrine to digital searches.	18
2.	Courts should impose use restrictions on seized data.	19

D. The search that turned up the relevant evidence in this case violated the
Fourth Amendment. 20

IV. CONCLUSION..... 24

TABLE OF AUTHORITIES

CASES

<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	6
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	6, 9
<i>Burns v. United States</i> , 235 A.3d 758 (D.C. 2020)	11
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	4, 6, 9
<i>Carroll v. United States</i> , 267 U.S. 132 (1925).....	9
<i>Doe v. Prosecutor</i> , 566 F. Supp. 2d 862 (S.D. Ind. 2008).....	20
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001).....	5
<i>Florida v. Harris</i> , 568 U.S. 237 (2013).....	6
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	6
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	8
<i>In re [REDACTED]@gmail.com</i> , 62 F. Supp. 3d 1100 (N.D. Cal. 2014).....	14, 20
<i>In re Search of Google Email Accounts identified in Attachment A</i> , 92 F. Supp. 3d 944 (D. Alaska 2015)	14
<i>In re Search Warrant</i> , 71 A.3d 1158 (Vt. 2012).....	20
<i>In re United States of America's Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunniss</i> , 770 F. Supp. 2d 1138 (W.D. Wash. 2011).....	13
<i>Johnson v. United States</i> , 333 U.S. 10 (1948).....	20
<i>Kentucky v. King</i> , 563 U.S. 452 (2011).....	6
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	9
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	7
<i>Nicholson v. City of Los Angeles</i> , 935 F.3d 685 (9th Cir. 2019)	21

1	<i>People v. Frank</i> , 38 Cal. 3d 711 (1985)	7
2	<i>People v. Hughes</i> , 958 N.W.2d 98 (Mich. 2020)	9
3	<i>People v. Musha</i> , 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020)	12
4	<i>Riley v. California</i> , 573 U.S. 373 (2014)	passim
5	<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	6
6	<i>State v. Bock</i> , 485 P.3d 931 (Or. App. 2021)	13, 18
7	<i>State v. Maddox</i> , 98 P.3d 1199 (Wash. 2004)	21
8	<i>State v. Mansor</i> , 421 P.3d 323 (Or. 2018)	10, 19
9	<i>State v. McLawhorn</i> , 2020 WL 6142866 (Tenn. Crim. App. 2020)	12
10	<i>Taylor v. State</i> , 260 A.3d 602 (Del. 2021)	13
11	<i>United States v. Abboud</i> , 438 F.3d 554 (6th Cir. 2006)	14
12	<i>United States v. Bishop</i> , 338 F.3d 623 (6th Cir. 2003)	19
13	<i>United States v. Bizier</i> , 111 F.3d 214 (1st Cir. 1997)	21
14	<i>United States v. Bowling</i> , 900 F.2d 926 (6th Cir. 1990)	21
15	<i>United States v. Cardwell</i> , 680 F.2d 75 (9th Cir. 1982)	7
16	<i>United States v. Comprehensive Drug Testing, Inc. (CDT)</i> , 621 F.3d 1162 (9th Cir. 2010)	3, 8, 20
17	<i>United States v. Diaz</i> , 841 F.2d 1 (1st Cir. 1988)	14
18	<i>United States v. Diggs</i> , 544 F.2d 116 (3d Cir. 1976)	20
19	<i>United States v. Drebin</i> , 557 F.2d 1316 (9th Cir. 1977)	7
20	<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	10
21	<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	6, 7

1	<i>United States v. Hillyard</i> , 677 F.2d 1336 (9th Cir. 1982)	7
2	<i>United States v. Jacobs</i> , 986 F.2d 1231 (8th Cir. 1993)	21
3	<i>United States v. Jones</i> , 565 U.S. 400 (2012).....	9
4	<i>United States v. Kow</i> , 58 F.3d 423 (9th Cir. 1995)	7
5	<i>United States v. Lopez</i> , 482 F.3d 1067 (9th Cir. 2007)	21
6	<i>United States v. Marin-Buitrago</i> , 734 F.2d 889 (2d Cir. 1984)	21
7	<i>United States v. Morgan</i> , 743 F.2d 1158 (6th Cir. 1984)	20
8	<i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021)	12
9	<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)	10
10	<i>United States v. Payton</i> , 573 F.3d 859 (9th Cir. 2009)	4, 5
11	<i>United States v. Shipp</i> , 392 F. Supp. 3d 300 (E.D.N.Y. 2019)	5, 12
12	<i>United States v. Stabile</i> , 633 F.3d 219 (3d Cir. 2011)	15
13	<i>United States v. Stetkiw</i> , No. 18-20579, 2019 WL 2866516 (E.D. Mich. July 3, 2019).....	10, 11
14	<i>United States v. Stubbs</i> , 873 F.2d 210 (9th Cir. 1989)	7
15	<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010)	5
16	<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017)	12, 13
17	<i>United States v. Williams</i> , 592 F.3d 511 (4th Cir. 2010)	15
18	OTHER AUTHORITIES	
19	Apple, <i>Compare Mac Models</i>	4
20	Apple, <i>macOS User Guide: Set up users, guests, and groups on Mac</i>	14
21	Christina M. Schuck, Note, <i>A Search for the Caselaw to Support the Computer Search</i> “Guidance” in <i>United States v. Comprehensive Drug Testing</i> , 16 Lewis & Clark L. Rev. 741 (2012)	19

1	David H. Angeli & Christina M. Schuck, <i>The Plain View Doctrine and Computer Searches: Balancing Law Enforcement’s Investigatory Needs with Privacy Rights in the Digital Age</i> , 34 Champion 18 (Aug. 2010)	19
2	Emily Berman, <i>Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt</i> , 68 Emory L.J. 49 (2018).....	11
3	Karen Kent et al., <i>Guide to Integrating Forensic Techniques Into Incident Response: Recommendations of the National Institute of Standards and Technology</i> , NIST SP No. 800-86 (Aug. 2006)	16
4	LexisNexis, <i>How Many Pages in a Gigabyte</i> (2007)	4
5	Microsoft, <i>Create a user account in Windows</i>	14
6	Microsoft, <i>Search for eDiscovery Activities in the Audit Log</i> , Microsoft Docs (Jan. 7, 2022)	16
7	Orin Kerr, <i>Executing Warrants for Digital Evidence</i> , 48 Tex. Tech. L. Rev. 1 (2015)	19
8	Press Release, Black Bag, BlackBag Announces Release of BlackLight 2019 R2 (Sept. 5, 2019).....	17
9	Rebecca Lipman, <i>Protecting Privacy with Fourth Amendment Use Restrictions</i> , 25 Geo. Mason L. Rev. 412 (2018)	19
10	Upturn, <i>Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones</i> (Oct. 2020).....	17
11	CONSTITUTIONAL PROVISIONS	
12	U.S. Const. amend. IV	5, 22
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		

I. INTRODUCTION & SUMMARY OF ARGUMENT

Courts should apply longstanding rules governing and limiting warrants scrupulously in the context of digital searches because almost any search of a device’s digital data can easily morph into a search of all the data on the device—and the Fourth Amendment prohibits general warrants. Computers now house almost unimaginable amounts of private and sensitive information. That, plus the Fourth Amendment’s requirement that searches be both particular and narrow, means that courts must tie what officers can search and seize closely to the probable cause showing for the particular case. Modern courts have recognized this, imposing limits on the relevant categories of data that can be searched, ensuring that time frames apply to the data searched, and insisting on a close nexus between probable cause and the data to be searched. These limits are necessary to avoid police fishing expeditions long barred by the Fourth Amendment and to prevent police from exploiting the trove of sensitive digital data stored on computer hard drives, on cell phones, and in online accounts by searching information they are not entitled to search.

In this case, police discovery of the video evidence was unconstitutional for two reasons. First, at the time police discovered these videos, officers no longer had probable cause to search Holcomb’s computer for evidence of rape—and no warrant authorized a search for evidence of any other crime. Second, the warrant provision authorizing a search for evidence of “dominion and control” was overbroad. Adoption of the government’s argument that the provision justified a search of any and every file on Holcomb’s computer would set a dangerous precedent. Indeed, the government’s capacious interpretation would give law enforcement a code word with which it could turn every warrant into an unconstitutional general one. A search for evidence of “dominion and control”—a need that does not appear to even been at issue in this case because it

1 was clear and undisputed that the computer belonged to the defendant—can be limited by date
 2 range and file type, thereby ensuring that a search for evidence of a particular crime does not
 3 become a search of everything on a device.

4 **II. FACTS**

5 During the course of their investigation of Holcomb for allegedly raping complainant JJ
 6 on the evening of January 27, 2020, officers with the Burlington Police Department obtained a
 7 warrant, signed by Judge Riquelme of Skagit County Superior Court in Washington, to search
 8 the defendant’s desktop computer. Dkt. #35-1 at 45–46. The warrant was based on Judge
 9 Riquelme’s finding of probable cause to believe that the computer contained evidence of the
 10 alleged rape of JJ. *Id.* Specifically, police believed based on an interview with Holcomb that the
 11 computer contained video recordings of the night in question that would confirm or contradict
 12 JJ’s statements. *Id.* at 53–54. Thus, the warrant authorized police to search for:
 13

- 14 1. Evidence of communications to or from JJ and/or between JOHN HOLCOMB,
 15 JILL [] or JJ. This communication includes but is not limited to voicemails/audio
 16 recordings, SMS, MMS, emails, chats, social media posts/online forums, contact
 17 lists and call logs from June 1, 2019 to current.
- 18 2. Surveillance video or images depicting JJ or JOHN HOLCOMB and any other
 19 surveillance video or images from Jan 26th, 2020 to current.
- 20 3. Any location data including GPS coordinates from Jan 26th to current.
- 21 4. User search history from the devices to include but not limited to searched words,
 22 items, phrases, names, places, or images from Jan 26th 2020 to current.
- 23 5. Files artifacts or information including but not limited to, documents,
 24 photographs, videos, e-mails, social media posts, chats and internet cache that
 25 would show dominion and control for the devices.

26 *Id.* at 45–46.

Investigators searched the computer. On February 20, 2020, the forensic examiner determined that the relevant video “raised a legitimate question as to the credibility of the complaining witness’ statement.” *Id.* at 71. After informing the investigator and prosecutor of that fact, on the morning of February 21, the three men reviewed the relevant video evidence and agreed that there was no evidence that the defendant had raped JJ. *Id.* at 63, 69. Nevertheless, the prosecutor asked the forensic examiner to continue processing and reviewing data on other hard drives. *Id.* at 63. Later in the day on February 21, the examiner found videos depicting sexual assault of a minor from 2016 and earlier. *Id.* at 69; Dkt. #41 at 6.

Apparently understanding that their search had exceeded the bounds of the Fourth Amendment, local authorities bemoaned having engaged in a constitutional violation before dismissing their cases and referring the matter to the FBI for possible federal prosecution. Dkt. #35-1 at 77.

III. ARGUMENT

A. **Courts must scrupulously apply longstanding Fourth Amendment rules regarding limits on warrants to searches of digital information to ensure that digital searches do not morph into unconstitutional general searches.**

1. Computers and other digital devices contain an immense amount of private, sensitive data.

Digital information generated by today’s devices reveals individuals’ private matters far beyond what one could learn from physical analogs. *See Riley v. California*, 573 U.S. 373, 394 (2014). Indeed, computers contain far more information of an extremely personal nature than even the most capacious filing cabinet ever could. *See id.* at 394–95; *see also United States v. Comprehensive Drug Testing, Inc. (CDT)*, 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam). A digital device the size of a human palm can store practically unlimited quantities of

1 data, *id.*, and computer hard drives can store even more, *see, e.g., United States v. Payton*, 573
 2 F.3d 859, 861–62 (9th Cir. 2009).¹ Moreover, while our garages and desk drawers may fill all
 3 the way up with knickknacks, requiring periodic spring cleaning, digital data can pile up and
 4 persist indefinitely.

5 Because both computers and cell phones “collect[] in one place many distinct types of
 6 information”—for example, an address, a note, a prescription, a bank statement, or a video—
 7 digital data “reveal much more in combination than any isolated record,” *Riley*, 573 U.S. at 394,
 8 and they reveal much more about “an individual’s private interests or concerns.” *Id.* at 395.
 9 Thus, law enforcement access to electronically stored data exposes years’—even decades’—
 10 worth of personal information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018);
 11 *Riley*, 573 U.S. at 394. This combination of volume, depth, and longevity of personal
 12 information raises strong privacy risks because in aggregate, digital information reveals much
 13 more than the sum of each part. *See Riley*, 573 U.S. at 394.

14 In some cases, technology has also given law enforcement the ability to obtain previously
 15 unobtainable information, *Carpenter*, 138 S. Ct. at 2217–18, such as Internet browsing history,
 16 location history, medical records, extensive conversations in the form of email or text, privileged
 17 communications, and associational information. Courts have already recognized some of these
 18 categories of information as deserving of particularly stringent privacy protections. *See, e.g.,*
 19 *Riley*, 573 U.S. at 395–96 (search and browsing history “could reveal an individual’s private
 20 interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent
 21
 22
 23

24 ¹ Laptops sold in 2021 can store up to eight terabytes of information, the equivalent of more than
 25 5 billion pages of text. *See, e.g., Apple, Compare Mac Models*,
 26 <https://www.apple.com/mac/compare/>; LexisNexis, *How Many Pages in a Gigabyte* (2007),
<https://perma.cc/HN26-3ZVC>.

visits to WebMD”); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (medical tests);
United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) (email). As the Supreme Court has
 explained, the “immense storage capacity” of smartphones—and computers—allows them to
 function as “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries,
 albums, televisions, maps, or newspapers,” and to store extensive historical information related
 to each functionality. *Riley*, 573 U.S. at 393.

Indeed, the search of computer devices “would typically expose to the government far
 more than the most exhaustive search of a house,” not least because they “contain[] a broad array
 of private information *never* found in a home in any form” prior to the digital age. *Id.* at 396–97.
 As the Ninth Circuit has explained, “searches of computers therefore often involve a degree of
 intrusiveness much greater in quantity, if not different in kind, from searches of other
 containers.” *Payton*, 573 F.3d at 861–62.²

2. The Fourth Amendment requires that warrants to search digital data be
 scrupulously particular and narrow.

a. *Warrants must clearly limit what officers may seize and police
 searches must be designed to find relevant information whose
 seizure is supported by probable cause.*

The Fourth Amendment protects people against unreasonable searches and seizures by
 requiring that all search warrants be based on probable cause and describe with particularity the
 places and items to be seized and searched. US Const. amend. IV. These provisions are meant to

² In addition, searches of computers or other digital devices that are connected to the Internet
 present risks that law enforcement searching through a device could access more than locally
 stored physical media but online accounts, too. *See, e.g., United States v. Shipp*, 392 F. Supp. 3d
 300, 308 (E.D.N.Y. 2019) (Police access to social media accounts and online communications
 services present a “threat [that] is further elevated . . . because, perhaps more than any other
 location—including a residence, a computer hard drive, or a car—[they] provide[] a single
 window through which almost every detail of a person’s life is visible.”).

1 protect against general warrants, a hated English practice that allowed a general rummaging
2 through the papers and property of anybody suspected of a crime. *See Stanford v. Texas*, 379
3 U.S. 476, 481 (1965) (general warrants were “the worst instrument of arbitrary power . . . that
4 ever was found in an English law book”).

5 A police officer has probable cause to conduct a search when “the facts available to [him]
6 would ‘warrant a [person] of reasonable caution in the belief’” that contraband or evidence of a
7 crime is present. *Florida v. Harris*, 568 U.S. 237, 243 (2013). The probable cause requirement
8 protects people in two ways: it ensures there is adequate justification for a search, *see Arizona v.*
9 *Gant*, 556 U.S. 332, 345 (2009), and it limits the scope of the search based on the warrant, *see*
10 *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). This requirement serves the goal of the
11 Fourth Amendment “to place obstacles in the way of a too permeating police surveillance.”
12 *Carpenter*, 138 S. Ct. at 2214 (citation and quotation marks omitted).

13
14 Search warrants must also be particular and narrow in scope. *See, e.g., Stanford*, 379 U.S.
15 at 485 (“The requirement that warrants shall particularly describe the things to be seized makes
16 general searches under them impossible and prevents the seizure of one thing under a warrant
17 describing another.” (citation omitted)); *Berger v. New York*, 388 U.S. 41, 58 (1967) (“The
18 Fourth Amendment’s requirement that a warrant ‘particularly describ(e) the place to be searched,
19 and the persons or things to be seized,’ repudiated these general warrants and ‘makes general
20 searches . . . impossible and prevents the seizure of one thing under a warrant describing
21 another.’” (alteration in original)); *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (“[T]he
22 warrant . . . was deficient in particularity because it provided no description of the type of
23 evidence sought.”); *Kentucky v. King*, 563 U.S. 452, 459 (2011) (“a warrant may not be issued
24
25
26

1 unless probable cause is properly established and the scope of the authorized search is set out
2 with particularity.”).

3 The two requirements of “particularity and breadth” are similar, but distinct.

4 “Particularity is the requirement that the warrant must clearly state what is sought. Breadth deals
5 with the requirement that the scope of the warrant be limited by the probable cause on which the
6 warrant is based.” *Hill*, 459 F.3d at 973 (citations omitted). The particularity requirement is met
7 “if the warrant imposes a meaningful restriction upon the objects to be seized.” *United States v.*
8 *Cardwell*, 680 F.2d 75 (9th Cir. 1982); *People v. Frank*, 38 Cal. 3d 711, 724 (1985). The breadth
9 requirement is met if the warrant constrains invasive “fishing expeditions” by authorizing
10 searches only for evidence of a crime for which there is probable cause. *See Maryland v.*
11 *Garrison*, 480 U.S. 79, 84 (1987).

12 A search is unlawfully general where the accompanying warrant “le[aves] to the
13 executing officers,” rather than to the magistrate upon issuance, “the task of determining what
14 items f[a]ll within broad categories stated in the warrant” and where there were no clear
15 guidelines distinguishing between property which was subject to search from that which was not.
16 *United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (citing *United States v. Drebin*,
17 557 F.2d 1316, 1322–23 (9th Cir. 1977)); *see also United States v. Kow*, 58 F.3d 423, 427 (9th
18 Cir. 1995) (warrant listing fourteen categories of business records without limiting descriptions
19 such as names of companies involved in illegal scheme was not sufficiently particular); *United*
20 *States v. Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989) (lack of probable cause to seize all office
21 documents without reason to believe tax evasion permeated defendant’s entire business).
22
23
24
25
26

1 Police must search only within the parameters of the warrant, and only when there is
2 probable cause. If police violate the terms of the warrant, the search is unconstitutional, absent
3 some exception to the warrant requirement.

4 b. *Adhering to constitutional requirements about overbreadth and*
5 *particularity is especially important when officers search*
6 *electronic information.*

7 The particularity requirement is more easily understood when applied during searches of
8 physical spaces. For example, a valid warrant to search for a rifle in someone's home does not
9 allow officers to open a medicine cabinet where a rifle could not fit. *See, e.g., Horton v.*
10 *California*, 496 U.S. 128, 141 (1990). Circumventing that limitation was not only unlawful, but
11 often obvious.

12 When it comes to searches of digital information, physical distinctions are no longer a
13 clear guardrail. Computer hard drives and online services contain huge amounts of personal
14 information that will inevitably intermingle material that is entirely irrelevant to a criminal
15 investigation and, potentially, evidence of criminal behavior. As a result, in the digital age,
16 courts must take even greater care to ensure that digital searches do not “become a vehicle for
17 the government to gain access to data which it has no probable cause to collect.” *CDT*, 621 F.3d
18 at 1177. The need to search large quantities of electronic records “creates a serious risk that
19 every warrant for electronic information will become, in effect, a general warrant, rendering the
20 Fourth Amendment irrelevant.” *Id.* at 1176.

21 The Fourth Amendment's originating principles are more important than ever as guides
22 for courts tasked with balancing law enforcement's legitimate need to search for evidence of a
23 crime on one hand, and the countervailing prohibition against general warrants and their evils.
24 As technology lowers the barriers to extreme privacy invasions and investigatory overreach, the
25
26

1 Fourth Amendment ensures that the longstanding balance between the power and authority of the
 2 state and the privacy and liberty of the individual does not, either suddenly or through creep, fall
 3 constitutionally out of whack. *See, e.g., Berger*, 388 U.S. at 56 (“The need for particularity . . . is
 4 especially great in the case of eavesdropping” because such surveillance “involves an intrusion
 5 on privacy that is broad in scope.”).

6 In cases involving law enforcement’s use or exploitation of emerging technologies, the
 7 Fourth Amendment analysis asks whether the police conduct threatens to disrupt the traditional
 8 “relationship between citizen and government in a way that is inimical to democratic society.”
 9 *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (quotation marks
 10 omitted). This analysis “is informed by historical understandings ‘of what was deemed an
 11 unreasonable search and seizure when [the Fourth Amendment] was adopted.’” *Carpenter*, 138
 12 S. Ct. at 2214 (alteration in original) (quoting *Carroll v. United States*, 267 U.S. 132, 149
 13 (1925)); *see also Kyllo v. United States*, 533 U.S. 27, 34 (2001). Courts must ensure that
 14 technological innovation does not allow the government to encroach on the degree of privacy the
 15 Fourth Amendment was adopted to protect. *See Carpenter*, 138 S. Ct. at 2214 (cell-site location
 16 information); *Kyllo*, 533 U.S. at 34–35 (thermal imaging).

19 **B. In case after case, courts are imposing limits on warrants in recognition that**
 20 **probable cause to search or seize some data on a digital device cannot justify**
 21 **access to the totality of the device’s contents.**

22 Given the vast amounts of personal data stored on digital media, and all that can be
 23 gleaned from that data, a growing number of courts are making clear that strict limits on digital
 24 searches and seizures are crucial to preserve privacy. For example, the Michigan Supreme Court
 25 held in *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020), that police were not permitted to search
 26 the suspect’s digital data for evidence of a crime not identified in the warrant. Quoting *Riley*, the

1 court rejected the state’s extreme argument

2 that it is always reasonable for an officer to review the entirety of the digital data
3 seized pursuant to a warrant on the basis of the mere possibility that evidence may
4 conceivably be found anywhere on the device or that evidence might be
5 concealed, mislabeled, or manipulated. Such a *per se* rule would effectively
6 nullify the particularity requirement of the Fourth Amendment in the context of
7 cell-phone data and rehabilitate an impermissible general warrant that “would in
8 effect give police officers unbridled discretion to rummage at will among a
9 person’s private effects.”

10 *Id.* at 541–42 (quoting *Riley*, 573 U.S. at 399). Warrants require probable cause and particularity
11 precisely *because* searching for evidence of an unrelated crime is not permitted, even when the
12 object is lawfully seized. Like the *Hughes* court, other courts have begun to impose similar
13 limitations on digital searches. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir.
14 2013) (discussing the need for “heightened sensitivity to the particularity requirement in the
15 context of digital searches” due to the vast amount of information that digital devices contain);
16 *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store “a
17 huge array” of information “makes the particularity requirement that much more important”); *see*
18 *also State v. Mansor*, 421 P.3d 323, 326 (Or. 2018) (holding that “warrant[s] must identify, as
19 specifically as reasonably possible in the circumstances, the information to be searched for,
20 including, if relevant and available, the time period during which that information was created,
21 accessed, or otherwise used,” and that warrants must describe, to the greatest degree of
22 specificity possible, the data for which there exists probable cause so as to prevent law
23 enforcement from “rummaging” indiscriminately through the vast amount of sensitive
24 information stored on cell phones).

25 A district court case from Michigan helpfully illustrates how courts are now managing
26 these issues. In *United States v. Stetkiw*, the government alleged, and the court was concerned,
that “individuals might hide information in a way that forces a protocol-bound investigator to

1 overlook it.” No. 18-20579, 2019 WL 2866516, at *5 (E.D. Mich. July 3, 2019). Nevertheless,
 2 the court held that “an *ex ante* ‘minimization’ requirement can address concerns about potential
 3 Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of
 4 non-responsive [electronically stored information] encountered in a search.” *Id.* (citing Emily
 5 Berman, *Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt*, 68 Emory L.J.
 6 49, 55 (2018)). The court concluded that *ex ante* procedures would have several advantages:

7 First, it can minimize the need for *ex post* review of those procedures, which is
 8 often contentious as parties debate motions to suppress evidence in criminal cases.
 9 Second, it allows a magistrate judge to closely work with the Government to
 10 ensure its preferred procedures do not violate the Fourth Amendment. Third, it
 11 can promote the development of case law that can distinguish permissible and
 12 impermissible procedures to better protect Fourth Amendment rights. Finally, it
 13 could prevent situations where certain file locations are authorized for search by
 14 warrant, but the practical implications of that authorization create a general
 15 warrant without the magistrate judge’s knowledge.

16 *Id.* While the *Stetkiw* court did not maintain that *ex ante* protocols must be required in every
 17 case, it did suggest that in order to escape the need for such protocols, the government “should
 18 demonstrate that the level of probable cause to search [electronically stored information] is high
 19 enough to justify a search without minimization.” *Id.*

20 1. Courts can and should impose limitations on the categories of data to be
 21 searched on a digital device.

22 There is no need for, and the Fourth Amendment does not allow, “all-content” warrants
 23 demanding seizure of whatever account content or digital files might exist. Rather than issue
 24 “all-content” warrants, courts should authorize seizure only of relevant categories of data that are
 25 supported by probable cause. Looking for the right data, not for *any* data, is the only search plan
 26 that makes sense and complies with the Constitution. *See, e.g., Burns v. United States*, 235 A.3d
 758, 775 (D.C. 2020) (warrant authorizing search for categories of data for which there was no
 probable cause was “constitutionally intolerable”).

Thus, for example, probable cause to search for photographs does not amount to probable cause to search for web history. *People v. Musha*, 131 N.Y.S.3d 514, 683 (N.Y. Sup. Ct. 2020); *see also United States v. Morton*, 984 F.3d 421 (5th Cir. 2021) (government properly obtained a warrant to search a cell phone for text messages, call logs, and contacts, but that warrant did not establish probable cause to believe the evidence would be in the form of photographs, which were therefore suppressed), *vacated and reh’g en banc granted*, 996 F.3d 754 (5th Cir. May 18, 2021). And probable cause to determine whether a suspect’s phone had a flashlight function does not authorize general rummaging through the phone’s entire contents. *State v. McLawhorn*, No. M2018-02152-CCA-R3-CD, 2020 WL 6142866, at *24–*26 (Tenn. Crim. App. Oct. 20, 2020).

Along these lines, one federal court rejected a search warrant that sought an individual’s Facebook account information that went far beyond the types of information likely to provide evidence of the specific crime under investigation and were unconnected to probable cause. *See United States v. Shipp*, 392 F. Supp. 3d 300, 303–07 (E.D.N.Y. 2019) (search warrant to Facebook demanding all personal information, activity logs, photos and videos from the user as well as those posted by others that tag the suspect, all postings, private messages, and chats, all friend requests, groups and applications activity, all private messages and video call history, check-ins, IP logs, “likes,” searches, use of Facebook Marketplace, payment information, privacy settings, blocked users, and tech support requests).

Similarly, courts are rejecting warrants that use the phrase “including but not limited to” or list capacious categories of data, as the fifth provision of the warrant here does. For example, in *United States v. Wey*, 256 F. Supp. 3d 355 (S.D.N.Y. 2017), the Southern District of New York rejected a warrant to search multiple types and categories of information—all “financial records, notes, memoranda, records of internal and external communications, correspondence,

1 audio tapes[] and video tapes, [and] photographs,” among others, *id.* at 386 (quotation marks
2 omitted)—that merely pertained to the suspects. As the court explained, because every document
3 seized from the suspect pertains to the suspect, the warrants did not impose “meaningful
4 parameters on an otherwise limitless search of a defendant’s electronic media,” and they failed
5 “to link the evidence sought to the criminal activity supported by probable cause” *Id.* at 387.
6 Thus, the warrants did “not satisfy the particularity requirement.” *Id.*

7
8 Likewise, the Delaware Supreme Court recently rejected a warrant, on particularity
9 grounds, that permitted the search and seizure of “any/all data stored by whatever means.”
10 *Taylor v. State*, 260 A.3d 602, 609 (Del. 2021). The court explained that “[t]he free-ranging
11 search for anything ‘pertinent to the investigation’ undermines the essential protections of the
12 Fourth Amendment—that a neutral magistrate approve in advance, based on probable cause, the
13 places to be searched and the parameters of the search.” *Id.* at 616. Other courts have followed
14 suit. *See, e.g., State v. Bock*, 485 P.3d 931, 936 (Or. App. 2021) (warrant authorizing the search
15 of a cell phone for circumstantial evidence about the owner and any evidence related to
16 suspected criminal offenses, including unlawful firearm possession, was not sufficiently specific
17 under state constitution’s Fourth Amendment corollary); *In re United States of America’s*
18 *Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunniss*,
19 770 F. Supp. 2d 1138, 1139, 1150 (W.D. Wash. 2011) (application to search and seize “all
20 electronically stored information . . . contained in any digital devices seized from [defendant’s]
21 residence for evidence relating to the crimes of copyright infringement or trafficking in
22 counterfeit goods” was improper because it sought “the broadest warrant possible”).

23
24 Finally, information whose search is justified by probable cause must still be limited to
25 the types of data likely to reveal that information. Thus, if a warrant authorizes a search of digital
26

1 data to show ownership—or, like in this case, “dominion and control”—there will be other forms
 2 of searchable data more than capable of demonstrating ownership, as opposed to more private
 3 data that could disclose the same thing. For example, on a machine running the Windows
 4 operating system, the “User Accounts” menu displays users’ account name and associated email
 5 address, information directly relevant to who has access to the computer, as well as what files
 6 they can access.³ And on an Apple Mac laptop, the System Preferences “Users & Groups” and
 7 “Internet Accounts” menu lists similar data.⁴

8
 9 2. Courts should limit searches by time frame to ensure they do not expand
 beyond data relevant to the crime under investigation.

10 Warrants can easily limit data searches and seizures by time frame. For example, if an
 11 offense allegedly took place in June of 2019, police need not view videos from any other month,
 12 nor data from much before or after the date when ownership of the hard drives is relevant. *See*
 13 *United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (“Failure to limit broad descriptive
 14 terms by relevant dates, when such dates are available to the police, will render a warrant
 15 overbroad.” (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant
 16 overbroad when authorized seizure records before the first instance of wrongdoing mentioned in
 17 the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no
 18 warrant issued where government did not include a date limitation); *In re Search of Google*
 19 *Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application
 20 without date restriction denied as overbroad).
 21
 22
 23

24
 25 ³ See Microsoft, *Create a user account in Windows*, <https://support.microsoft.com/en-us/windows/create-a-user-account-in-windows-4fac6fd5-74c0-9737-69b8-6e77e00422dc>.

26 ⁴ See Apple, *macOS User Guide: Set up users, guests, and groups on Mac*, <https://support.apple.com/guide/mac-help/set-up-other-users-on-your-mac-mtusr001/mac>.

- 1 3. Forensic tools make it straightforward for law enforcement to narrow
 2 searches by file type, date range, and other limitations that adhere closely
 3 to probable cause.

4 Contrary to some government claims, officers need not perform a file-by-file review of
 5 the data on a suspect's computer in every case. Some prosecutors have argued and some courts
 6 have held that because criminals can hide or mislabel files, expansive searches of digital
 7 information are both practically necessary and permissible under the Fourth Amendment. *See,*
 8 *e.g., United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011); *see also United States v.*
 9 *Williams*, 592 F.3d 511, 521 (4th Cir. 2010).⁵ Indeed, the government here argues that any data
 10 on Holcomb's computer is fair game to prove dominion and control. Dkt. #41 at 13, 25–27. But
 11 these assertions are premised on an outmoded understanding of today's technology. Indeed,
 12 review of every file in suspects' online accounts or on their hard drives will often be
 13 counterproductive, for it is impractical for an investigator to manually review the hundreds of
 14 thousands of images, files, and messages stored there.

15 Instead, modern forensics tools, widely available today for both criminal investigations
 16 and e-discovery, can search data for file type, dates, and keywords, all without revealing the
 17 contents of non-responsive documents to a human reviewer.

18 Fortunately, various tools and techniques can be used to reduce the amount of
 19 data that has to be sifted through. Text and pattern searches can be used to
 20 identify pertinent data, such as finding documents that mention a particular
 21 subject or person, or identifying e-mail log entries for a particular e-mail address.
 22 Another helpful technique is to use a tool that can determine the type of contents

23 ⁵ In some cases, when a suspect is using sophisticated techniques to hide data, it may make sense
 24 to give officers increased leeway in their search to find potentially hidden information. But in
 25 such a scenario, there should be a probable cause showing of the actor's "sophisticated" nature—
 26 perhaps, for example, the suspect is a skilled computer programmer who knows how to
 manipulate data. But since the scope of a warrant must be limited by probable cause, if a suspect
 is not shown to be sophisticated, there will be no reason to believe that relevant evidence will be
 found in files or places not specifically connected to probable cause.

of each data file, such as text, graphics, music, or a compressed file archive. Knowledge of data file types can be used to identify files that merit further study, as well as to exclude files that are of no interest to the examination. There are also databases containing information about known files, which can also be used to include or exclude files from further consideration.

Karen Kent et al., *Guide to Integrating Forensic Techniques Into Incident Response: Recommendations of the National Institute of Standards and Technology*, NIST SP No. 800-86, § 3.2 (Aug. 2006), <https://perma.cc/Y2N7-K65R>.

Forensic tools may have a search history feature, just as eDiscovery tools do.⁶ Such query or audit logs facilitate a post-search review to ensure law enforcement complied with the dictates of the warrant. With such logs, judges could better understand the precise steps that law enforcement took when searching a cell phone. In particular, these logs could equip judges to better assess the reasonableness of the search technique and ascertain if the search was sufficiently narrowly tailored to the warrant. If courts were to insist upon the production of digital audit logs created by the forensic tool upon the return of a search warrant, tool vendors that do not already provide this functionality would rapidly develop this feature.

There are many such products on the market and available to law enforcement at the state and local level, as well as to the FBI. Forensic ToolKit and Cellebrite are just two examples. The Blacklight tool claims to categorize both still images and videos as related to Alcohol, Child Sexual Abuse Material (CSAM), Currency, Drugs, Extremism, Gambling, Gore, Porn,

⁶ See, e.g., Microsoft, *Search for eDiscovery Activities in the Audit Log*, Microsoft Docs (Jan. 7, 2022), <https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide> (explaining that content search and eDiscovery-related activities are logged in the audit log when creating, starting, and editing Content searches, and performing search actions, such as previewing, exporting, and deleting search results, among other activities).

Swim/Underwear, and Weapons.⁷ Research by the firm Upturn shows that mobile device forensic tools are widely available even to smaller law enforcement agencies, which either purchase them outright, obtain them through federal grants, or work with larger local law enforcement agencies that conduct extractions of data at the smaller agencies' request.⁸

In sum, forensic search tools can make searches limited by date and file type workable, while also being effective for law enforcement. Proper warrants and judicial oversight can ensure that these powerful tools are used in ways that reduce rummaging, limit law enforcement agents' exposure to non-responsive information, and enable judicial oversight and auditing of the search process. Certainly, limiting searches by file category or type will not always be possible—but it often is, and in those situations, this Court should require that warrants indicate, and officers observe, that limitation.

C. Courts have additional options to ensure that overseizures of data are not exploited in ways that give law enforcement a windfall simply because potential evidence is digital in nature.

When seizing hard drives or cell phone, investigators obtain more data that can lawfully be searched under a warrant's authority. If the government is permitted to seize materials beyond the scope of a properly narrow warrant, but then later exploit the overseizure by examining any files or videos it wishes—as happened in this case—it undermines the particularity requirement so essential to ensuring that searches and seizures are constitutional.

⁷ Press Release, BlackBag, BlackBag Announces Release of BlackLight 2019 R2 (Sept. 5, 2019), <https://www.blackbagtech.com/press-releases/blackbag-announces-release-of-blacklight-2019-r2>.

⁸ See Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020), <https://perma.cc/7DCK-PGMQ>.

1 Because of this, courts can and should issue warrants that ensure that law enforcement's
 2 subsequent searches of that data will be cabined to probable cause. In other words, courts should
 3 ensure that electronic searches do not become data windfalls for law enforcement.

4 1. Courts should strictly limit any applications of the plain view doctrine to
 5 digital searches.

6 In its opposition brief, the government suggests that the search of the video evidence in
 7 this case would be justified by the plain view doctrine. Dkt. #41 at 13. But the plain view
 8 doctrine, especially if applied as broadly as the government suggests could be done here, would
 9 seriously threaten to turn every digital search into an unconstitutional general one. Indeed, that
 10 threat is present here, because the government asserts that even if investigators have ulterior
 11 motives in conducting their searches, they can search every video (and other files) and use
 12 whatever they find. *Id.* at 14.

14 To avoid unconstitutional general searches, the Fourth Amendment must ensure that
 15 investigators do not take advantage of the unique properties of digital storage and reap a windfall
 16 by opening non-responsive files and discovering evidence of some other crime, as took place
 17 here. The plain view doctrine developed in cases involving physical-world searches, where
 18 evidence is tangible and discrete. But electronic searches are a poor fit for the plain view
 19 exception because the justifications underlying the exception are, by and large, absent in this
 20 context. *See e.g., Bock*, 483 P.3d 931 (holding plain view exception cannot be reconciled with
 21 the Oregon Constitution's Fourth Amendment analogue in the context of electronic searches).
 22 First, officer safety is not implicated in a controlled environment like an off-site forensics
 23 laboratory. *See generally* David H. Angeli & Christina M. Schuck, *The Plain View Doctrine and*
 24 *Computer Searches: Balancing Law Enforcement's Investigatory Needs with Privacy Rights in*
 25
 26

1 *the Digital Age*, 34 *Champion* 18, 23 (Aug. 2010). Unlike a physical object, such as a knife or
 2 gun, *see, e.g., United States v. Bishop*, 338 F.3d 623, 628–29 (6th Cir. 2003), the digital data
 3 stored on a computer hard drive can physically endanger no one. *See Riley*, 573 U.S. at 386–87.
 4 Second, evidence preservation is not at risk in a typical computer search, which normally begins
 5 with seizure of the computer and its data and extraction of the data stored on the hard drive.
 6 Third, where the computer hard drive is preserved pending execution of the warrant, the police
 7 have ample time to obtain additional warrants (say, for permission to expand the search or for
 8 evidence of an unrelated crime) without risking evidence destruction. *See, e.g., Christina M.*
 9 *Schuck*, Note, *A Search for the Caselaw to Support the Computer Search “Guidance” in United*
 10 *States v. Comprehensive Drug Testing*, 16 *Lewis & Clark L. Rev.* 741, 760–61 (2012).

12 2. Courts should impose use restrictions on seized data.

13 To ensure that broad digital searches adhere to Fourth Amendment principles, courts
 14 should exclude evidence police stumble upon, and impose a general use restriction on any non-
 15 responsive data obtained in an electronic search and seizure. *Mansor*, 421 P.3d at 343–45
 16 (holding that the State may not use information obtained in a computer search in a prosecution if
 17 the warrant did not authorize the search for that information, unless some other warrant
 18 exception applies); *see also* Orin Kerr, *Executing Warrants for Digital Evidence*, 48 *Tex. Tech.*
 19 *L. Rev.* 1, 8 (2015); Rebecca Lipman, *Protecting Privacy with Fourth Amendment Use*
 20 *Restrictions*, 25 *Geo. Mason L. Rev.* 412 (2018). The doctrinal reasoning behind this view is
 21 that, although the seizure of non-responsive files is reasonable when needed to effectuate the
 22 search for responsive files, retention of the files is an ongoing seizure. While initially justified,
 23 the subsequent use of seized non-responsive files transforms the nature of the seizure and renders
 24 it constitutionally unreasonable. *Id.* at 25–29. Even when a search is reasonable, the government

1 should be required to delete materials that were not the object of the search once they have been
2 segregated. *See CDT*, 621 F.3d at 1177 (discussing the need to segregate nonresponsive
3 information).

4 Courts now are implementing versions of these solutions. For example, in Vermont,
5 magistrates may design and supervise “targeted searches” by “restricting law enforcement’s
6 search to those items that met certain parameters based on dates, types of files, or the author of a
7 document.” *See In re Search Warrant*, 71 A.3d 1158, 1184 (Vt. 2012); *see also In re*
8 *[REDACTED]@gmail.com*, 62 F. Supp. 3d at 1104 (denying a search warrant for a particular
9 email account because “there is no date restriction of any kind”).

11 As one federal judge put it, “[i]t is almost always possible to characterize the Fourth
12 Amendment as an inconvenience to law enforcement officials as they carry out their vital
13 duties,” but “[t]hat inconvenience . . . is one of the fundamental protections that separates the
14 United States of America from totalitarian regimes.” *Doe v. Prosecutor*, 566 F. Supp. 2d 862,
15 887 (S.D. Ind. 2008). *See also Johnson v. United States*, 333 U.S. 10, 15 (1948); *United States v.*
16 *Morgan*, 743 F.2d 1158, 1163–64 (6th Cir. 1984); *United States v. Diggs*, 544 F.2d 116, 130 (3d
17 Cir. 1976).

19 **D. In this case, the search that turned up the relevant evidence violated the**
20 **Fourth Amendment.**

21 The government’s search in this case was unconstitutional under the Fourth Amendment
22 for two reasons. First, no probable cause existed to continue searching Holcomb’s computer.
23 And second, the warrant at issue did not authorize and could not have authorized the search that
24 uncovered the video evidence at issue in this case.

1 First, at the point that the prosecution team realized the video of Holcomb’s sexual
 2 encounter with JJ was exculpatory and that he had committed no crime, they should have
 3 stopped their search. At that point, there was no longer probable cause, and probable cause is
 4 essential in defining a permissible scope of searches of electronic data. *See supra* Part III.A.2.a.

5 Probable cause must exist not only at the time law enforcement obtains a warrant, but at
 6 the time the warrant is executed as well. Where a search warrant is issued on probable cause,
 7 changed circumstances or new information can weaken or even entirely negate a prior
 8 determination of probable cause. *See United States v. Bizier*, 111 F.3d 214, 219 (1st Cir. 1997)
 9 (intervening information can weaken probable cause); *United States v. Jacobs*, 986 F.2d 1231,
 10 1235 (8th Cir. 1993) (finding new information can negate prior determination of probable cause).
 11 Execution of a warrant violates the Fourth Amendment if, between the time of issuance and the
 12 time of execution, probable cause becomes stale or dissipates. Police “may not disregard facts
 13 tending to dissipate probable cause.” *Nicholson v. City of Los Angeles*, 935 F.3d 685 (9th Cir.
 14 2019). When new circumstances call into question an original finding of probable cause, the
 15 officer must bring the new information to the issuing magistrate’s attention. *United States v.*
 16 *Bowling*, 900 F.2d 926, 933 (6th Cir. 1990); *State v. Maddox*, 98 P.3d 1199, 1203–04 (Wash.
 17 2004). An officer has a duty to report the new information to the magistrate if “the information is
 18 material to the magistrate’s determination of probable cause.” *United States v. Marin-Buitrago*,
 19 734 F.2d 889, 894 (2d Cir. 1984). For example, there may initially be probable cause justifying
 20 an arrest, but additional information obtained at the scene may indicate that there is less than a
 21 fair probability that the defendant has committed or is committing a crime. In such cases,
 22 execution of the arrest or continuation of the arrest is illegal. *United States v. Lopez*, 482 F.3d
 23 1067, 1073 (9th Cir. 2007).
 24
 25
 26

1 Here, the prosecutor’s failure to call off the search resulted in an invasive search without
 2 probable cause, or at least without the magistrate’s independent finding that the Fourth
 3 Amendment requires. U.S. Const. amend. IV. The forensic examiner, at least, appears to have
 4 viewed videos depicting Holcomb having sex with his wife while searching despite knowing that
 5 the probable cause that had formed the basis of the warrant was stale.

6 Second, the government argues that the investigators’ examination of the videos at issue
 7 in this case was lawful because the warrant authorized searches for evidence of “dominion and
 8 control.” Dkt. #41 at 12–16. However, a need to search for evidence of “dominion and control”
 9 over a computer does not and cannot justify police examination of any or all information stored
 10 there. *See supra* Part III.C.1–2. Otherwise, mere inclusion of the phrase “dominion and control”
 11 would permit an essentially boundless examination of all of a computer’s contents, threatening to
 12 turn all digital searches into unconstitutional general ones.

13 As an initial matter, there was really no question in this case that the computer belonged
 14 to the Defendant. The record is replete with police references to the device at issue as the
 15 Defendant’s computer, and the police seized it based on his consent—something that would have
 16 been improper without a reason to believe it was his machine. Dkt. #49 at 17–18 & n.12. Even if
 17 dominion and control were genuinely an issue in the case, a warrant permitting a search of “Files
 18 artifacts or information (sic) including but not limited to, documents” and other broad categories
 19 is overbroad and not sufficiently particularized. *See id.* at 13–18.⁹

20 Moreover, as explained above, *see supra* Part III.C.1–2, the “dominion and control”
 21
 22
 23
 24

25 ⁹ Oddly, the government asserts that “the warrant issued did not include the ‘including, but not
 26 limited to’ language that Holcomb finds so problematic.” Dkt. #41 at 24. It does. Dkt. #35-1 at
 46.

1 authorization should have included a date range relevant to the case, as did the other warrant
2 provisions. For example, it should have limited searches to indicia of dominion and control in
3 June of 2019. It also should have identified specific, narrow categories of data closely tied to
4 ownership and usage. Officers could have been limited to searching system preferences for a list
5 of user accounts, which generally include identifiers such as an email address. They could have
6 looked to see what email or social network accounts were logged in on the machine (without
7 review the contents of those messages), or what logins were stored in a password saver. Any of
8 these categories of data, which show that a defendant logs in to the computer and checks his
9 email there, are more probative of ownership, custody, and control of the computer than merely
10 appearing in a video recorded by cameras in the home. After all, JJ and Jill appeared in videos,
11 but it was not their computer.
12

13 Date, file type, and other limitations are crucial in the digital age, and they are easy for
14 courts to impose and police to follow. Other parts of the warrant properly used date limitations
15 that should have ensured that old emails or photographs contained on a seized device were not
16 unnecessarily searched. Similar limitations on warrant clause five should have prevented law
17 enforcement from encroaching upon private information whose review was *not* connected to
18 probable cause of rape and discovering the relevant evidence in this case.
19

20 Indeed, police in this case may have viewed some of the most private and intimate
21 information imaginable, videos of the defendant and his wife having sex, going back as far as
22 2015, as well as conversations between the two in which they discussed their sex life. Dkt. #49 at
23 18, 38. But law enforcement had no legitimate authority to look at that information in order to
24 investigate the defendant for a rape that occurred in January of 2020.
25
26

IV. CONCLUSION

For these reasons, the Court should hold that the search in this case was unconstitutional.

DATED this 15th day of April, 2022.

AMERICAN CIVIL LIBERTIES UNION OF
WASHINGTON FOUNDATION

By: s/Nancy Talner

Nancy L. Talner, WSBA 11196
P.O. Box 2728
Seattle, WA 98111
Tel: (206) 624-2184
E-mail: talner@aclu-wa.org

Counsel for Amici Curiae

AMERICAN CIVIL LIBERTIES UNION
FOUNDATION

Brett Max Kaufman*
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
E-mail: bkaufman@aclu.org

Jennifer Stisa Granick*
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
Email: jgranick@aclu.org

**Admitted Pro Hac Vice*